UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/810,696	03/29/2004	Masami Nasu	251145US2	1217

22850 7590 03/18/2008

OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
LOUIE, OSCAR A	

ART UNIT	PAPER NUMBER
2136	

NOTIFICATION DATE	DELIVERY MODE
03/18/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

Office Action Summary	Application No.	Applicant(s)	
	10/810,696	NASU, MASAMI	
	Examiner	Art Unit	
	OSCAR A. LOUIE	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 December 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-56* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-56* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This final action is in response to the amendment filed on 12/27/2007. In light of the applicant's amendments, the examiner hereby withdraws his previous 35 U.S.C. 101 rejections regarding Claims 22 & 50 and 35 U.S.C. 112 2nd paragraph rejections regarding Claims 1, 14, 22, 30, 43, & 50. Claims 1-56 are pending and have been considered as follows.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1-56 are rejected under 35 U.S.C. 102(b) as being anticipated by Frailong et al. (US-6230194-B1).

Claim 1:

Frailong et al. disclose a software update device configured to communicate with a target update device via a network comprising,

- "a certification information setting unit configured to generate a first certification information" (i.e. "Each remote management server receives an RSA key pair along with a public key Certificate signed by the RSA Head-End CA") [column 19 lines 50-52];

- "transmit the first certification information to the target update device via a first communication protocol over the network" (i.e. "The RSA Hardware Certificate 1416 is used in SSL communications where the identity of the gateway interface device needs to be proven, for example when opening a session to a remote management server") [column 19 lines 39-41];
- "a certification requesting unit configured to transmit a second certification information to the target update device" (i.e. "The second level of certificate key hierarchy for the hardware aspect of the gateway interface device is a manufacturing Certificate Authority, referred to as the RSA Hardware CA 1412") [column 19 lines 18-21];
- "request the target update device to execute a certification process with the first and second certification information" (i.e. "Like the RSA system, the DSA system also includes second and third level key certificates for the gateway interface device") [column 19 lines 61-63];
- "a transmitting unit configured to transmit an update software that updates a software of the target update device to the target update device via a second communication protocol over the network when the certification process succeeds via the first communication protocol" (i.e. "transmitting files using the TCP/IP file transfer protocol (FTP). These FTP sites provide the upgrade package for download to client networks which request the upgrade") [column 15 lines 18-21];

- "the second communication protocol having a process load less than that of the first communication protocol" (i.e. "transmitting files using the TCP/IP file transfer protocol (FTP). These FTP sites provide the upgrade package for download to client networks which request the upgrade") [column 15 lines 18-21].

Claim 2:

Frailong et al. disclose a software update device configured to communicate with a target update device via a network, as in Claim 1 above, further comprising,

- "a certification information invalidation requesting unit configured to request the target update device to invalidate the first certification information subsequent to the transmittal of the update software" (i.e. "update mechanism using Certificate Revocation Lists. A Certificate Revocation List is a time-valued list of serial numbers signed by a Certification Authority") [column 20 lines 11-13].

Claim 3:

Frailong et al. disclose a software update device configured to communicate with a target update device via a network, as in Claim 1 above, further comprising,

- "the software of the target update device is updated when requested by an external unit" (i.e. "If the gateway interface device verifies that an upgrade is both possible and appropriate, the gateway interface device executes the install script to apply the upgrade at the time specified by the apply time window, step 1020") [column 16 lines 14-17].

Claim 4:

Frailong et al. disclose a software update device configured to communicate with a target update device via a network, as in Claim 3 above, further comprising,

- "a notification unit configured to notify a result of updating the software of the target update device to the external unit" (i.e. "If, however, in step 1022 the gateway interface device determines that the upgrade and reboot were successful, the gateway interface device then executes the post-install script and notifies the remote management server of the upgraded status, step 1030") [column 16 lines 36-40].

Claim 5:

Frailong et al. disclose a software update device configured to communicate with a target update device via a network, as in Claim 1 above, further comprising,

- "the first communication protocol is SSL" (i.e. "SSL-secured access to the administrative web server") [column 19 lines 43-44].

Claim 6:

Frailong et al. disclose a software update device configured to communicate with a target update device via a network, as in Claim 1 above, further comprising,

- "the second communication protocol is FTP" (i.e. "transmitting files using the TCP/IP file transfer protocol (FTP). These FTP sites provide the upgrade package for download to client networks which request the upgrade") [column 15 lines 18-21].

Claim 7:

Frailong et al. disclose a software update device configured to communicate with a target update device via a network, as in Claim 1 above, further comprising,

- "data transmitted via the first communication protocol is encoded" (i.e. "SSL-secured access to the administrative web server") [column 19 lines 43-44];
- "data transmitted via the second communication protocol is not encoded" (i.e. "transmitting files using the TCP/IP file transfer protocol (FTP). These FTP sites provide the upgrade package for download to client networks which request the upgrade") [column 15 lines 18-21].

Claim 8:

Frailong et al. disclose a software update system comprising,

- "a software update device" (i.e. "remote management server") [column 14 line 64];
- "a target update device in communication with the software update device" (i.e. "gateway interface device") [column 14 line 64];
- "wherein the software update device comprises: a certification information setting unit configured to generate a first certification information" (i.e. "Each remote management server receives an RSA key pair along with a public key Certificate signed by the RSA Head-End CA") [column 19 lines 50-52];

- "transmit the first certification information to a target update device via a first communication protocol over the network" (i.e. "The RSA Hardware Certificate 1416 is used in SSL communications where the identity of the gateway interface device needs to be proven, for example when opening a session to a remote management server") [column 19 lines 39-41];
- "a certification requesting unit configured to transmit a second certification information to the target update device" (i.e. "The second level of certificate key hierarchy for the hardware aspect of the gateway interface device is a manufacturing Certificate Authority, referred to as the RSA Hardware CA 1412") [column 19 lines 18-21];
- "request the target update device to execute a certification process with the first and second certification information" (i.e. "Like the RSA system, the DSA system also includes second and third level key certificates for the gateway interface device") [column 19 lines 61-63];
- "a transmitting unit configured to transmit an update software for updating a software of the target update device to the target update device via a second communication protocol over the network when the certification process succeeds via the first communication protocol" (i.e. "transmitting files using the TCP/IP file transfer protocol (FTP). These FTP sites provide the upgrade package for download to client networks which request the upgrade") [column 15 lines 18-21];

- "the second communication protocol having a process load less than that of the first communication protocol" (i.e. "transmitting files using the TCP/IP file transfer protocol (FTP). These FTP sites provide the upgrade package for download to client networks which request the upgrade") [column 15 lines 18-21];
- "wherein the target update device comprises: a memory unit configured to store the first certification information" (i.e. "The gateway interface device stores two root RSA public key certificates and two root DSA public key certificates, with the corresponding private keys") [column 18 lines 57-58];
- "a certification unit configured to execute the certification process by using the first and second certification information when requested to execute the certification process" (i.e. "Like the RSA system, the DSA system also includes second and third level key certificates for the gateway interface device") [column 19 lines 61-63];
- "return a result of the certification process to the software update device" (i.e. "Like the RSA system, the DSA system also includes second and third level key certificates for the gateway interface device") [column 19 lines 61-63];
- "an updating unit configured to receive the update software when the certification process succeeds" (i.e. "transmitting files using the TCP/IP file transfer protocol (FTP). These FTP sites provide the upgrade package for download to client networks which request the upgrade") [column 15 lines 18-21];

- "update the software of the target update device" (i.e. "If the gateway interface device verifies that an upgrade is both possible and appropriate, the gateway interface device executes the install script to apply the upgrade at the time specified by the apply time window, step 1020") [column 16 lines 14-17].

Claim 9:

Frailong et al. disclose a software update system, as in Claim 8 above, further comprising,

- "wherein the software update device further comprises a certification information invalidation requesting unit configured to transmit an invalidation request to invalidate the first certification information to the target update device subsequent to the transmittal of the update software" (i.e. "update mechanism using Certificate Revocation Lists. A Certificate Revocation List is a time-valued list of serial numbers signed by a Certification Authority") [column 20 lines 11-13];
- "wherein the target update device further comprises a certification information invalidating unit configured to invalidate the first certification information when receiving the invalidation request" (i.e. "update mechanism using Certificate Revocation Lists. A Certificate Revocation List is a time-valued list of serial numbers signed by a Certification Authority") [column 20 lines 11-13].

Claim 10:

Frailong et al. disclose a software update system, as in Claim 8 above, further comprising,

- "wherein the target update device further comprises: a restarting unit configured to restart the target update device after the software is updated by the updating unit" (i.e. "Once the gateway interface device has executed the upgrade, it performs a reboot so that it boots up in the upgraded state") [column 16 lines 23-25];
- "a start notification transmitting unit configured to transmit a start notification informing that the target update device is started to the software update device when the target update device is started" (i.e. "If the gateway interface device verifies that an upgrade is both possible and appropriate, the gateway interface device executes the install script to apply the upgrade at the time specified by the apply time window, step 1020") [column 16 lines 14-17];
- "a version information transmitting unit configured to transmit version information of the target update device in response to a request from the software update device" (i.e. "recording the upgraded version number in appropriate places for the configuration manager") [column 16 lines 44-46];
- "where the software update device further has a version information unit configured to obtain the version information by requesting the target update device to transmit the version information when the start notification is received after the transmittal of the update software" (i.e. "recording the upgraded version number in appropriate places for the configuration manager") [column 16 lines 44-46];

- "confirm the update by comparing with version information of the transmitted update software" (i.e. "recording the upgraded version number in appropriate places for the configuration manager") [column 16 lines 44-46].

Claim 11:

Frailong et al. disclose a software update system, as in Claim 8 above, further comprising,

- "the first communication path is a communication protocol is SSL" (i.e. "SSL-secured access to the administrative web server") [column 19 lines 43-44].

Claim 12:

Frailong et al. disclose a software update system, as in Claim 8 above, further comprising,

- "the second communication path is a communication protocol is FTP" (i.e. "transmitting files using the TCP/IP file transfer protocol (FTP). These FTP sites provide the upgrade package for download to client networks which request the upgrade") [column 15 lines 18-21].

Claim 13:

Frailong et al. disclose a software update system, as in Claim 8 above, further comprising,

- "data transmitted via the first communication protocol is encoded" (i.e. "SSL-secured access to the administrative web server") [column 19 lines 43-44];
- "data transmitted via the second communication protocol is not encoded" (i.e. "transmitting files using the TCP/IP file transfer protocol (FTP). These FTP sites provide the upgrade package for download to client networks which request the upgrade") [column 15 lines 18-21].

Claims 14 & 22:

Frailong et al. disclose a software update method using a software update device configured to and a computer readable storage medium encoded with computer executable instructions, which when executed by a computer, cause the computer to perform a method that controls a software update device configured to communicate with a target update device via a network comprising,

- "generating a first certification information" (i.e. "Each remote management server receives an RSA key pair along with a public key Certificate signed by the RSA Head-End CA") [column 19 lines 50-52];
- "transmitting the first certification information to the target update device via a first communication protocol over the network" (i.e. "The RSA Hardware Certificate 1416 is used in SSL communications where the identity of the gateway interface device needs to be proven, for example when opening a session to a remote management server") [column 19 lines 39-41];
- "transmitting a second certification information to the target update device" (i.e. "The second level of certificate key hierarchy for the hardware aspect of the gateway interface device is a manufacturing Certificate Authority, referred to as the RSA Hardware CA 1412") [column 19 lines 18-21];
- "requesting the target update device to execute a certification process with the first and second certification information" (i.e. "Like the RSA system, the DSA system also includes second and third level key certificates for the gateway interface device") [column 19 lines 61-63];

- "transmitting an update software that updates a software of the target update device to the target update device via a second communication protocol over the network when the certification process succeeds" (i.e. "transmitting files using the TCP/IP file transfer protocol (FTP). These FTP sites provide the upgrade package for download to client networks which request the upgrade") [column 15 lines 18-21];
- "the second communication protocol having a process load less than that of the first communication protocol" (i.e. "transmitting files using the TCP/IP file transfer protocol (FTP). These FTP sites provide the upgrade package for download to client networks which request the upgrade") [column 15 lines 18-21].

Claims 15 & 23:

Frailong et al. disclose a software update method using a software update device configured to and a computer readable storage medium encoded with computer executable instructions, which when executed by a computer, cause the computer to perform a method that controls a software update device configured to communicate with a target update device via a network, as in Claims 14 & 22 above, further comprising,

- "a step of requesting the target update device to invalidate the first certification information subsequent to the transmittal of the update software" (i.e. "update mechanism using Certificate Revocation Lists. A Certificate Revocation List is a time-valued list of serial numbers signed by a Certification Authority") [column 20 lines 11-13].

Claims 16 & 24:

Frailong et al. disclose a software update method using a software update device configured to and a computer readable storage medium encoded with computer executable instructions, which when executed by a computer, cause the computer to perform a method that controls a software update device configured to communicate with a target update device via a network, as in Claims 14 & 22 above, further comprising,

- "the software of the target update device is updated when requested by an external unit" (i.e. "If the gateway interface device verifies that an upgrade is both possible and appropriate, the gateway interface device executes the install script to apply the upgrade at the time specified by the apply time window, step 1020") [column 16 lines 14-17].

Claims 17 & 25:

Frailong et al. disclose a software update method using a software update device configured to and a computer readable storage medium encoded with computer executable instructions, which when executed by a computer, cause the computer to perform a method that controls a software update device configured to communicate with a target update device via a network, as in Claims 16 & 24 above, further comprising,

- "a step of notifying a result of updating the software of the target update device to the external unit" (i.e. "If, however, in step 1022 the gateway interface device determines that the upgrade and reboot were successful, the gateway interface device then executes the post-install script and notifies the remote management server of the upgraded status, step 1030") [column 16 lines 36-40].

Claims 18 & 26:

Frailong et al. disclose a software update method using a software update device configured to and a computer readable storage medium encoded with computer executable instructions, which when executed by a computer, cause the computer to perform a method that controls a software update device configured to communicate with a target update device via a network, as in Claims 14 & 22 above, further comprising,

- "receiving a start notification informing that the target update device is started" (i.e. "Once the gateway interface device has executed the upgrade, it performs a reboot so that it boots up in the upgraded state") [column 16 lines 23-25];
- "obtaining version information of the software of the target update device from the target update device when the start notification is received after the transmittal of the update software" (i.e. "recording the upgraded version number in appropriate places for the configuration manager") [column 16 lines 44-46];
- "confirming the update by comparing with version information of the transmitted update software" (i.e. "recording the upgraded version number in appropriate places for the configuration manager") [column 16 lines 44-46].

Claims 19 & 27:

Frailong et al. disclose a software update method using a software update device configured to and a computer readable storage medium encoded with computer executable instructions, which when executed by a computer, cause the computer to perform a method that controls a software update device configured to communicate with a target update device via a network, as in Claims 14 & 22 above, further comprising,

- "the first communication protocol is SSL" (i.e. "SSL-secured access to the administrative web server") [column 19 lines 43-44].

Claims 20 & 28:

Frailong et al. disclose a software update method using a software update device configured to and a computer readable storage medium encoded with computer executable instructions, which when executed by a computer, cause the computer to perform a method that controls a software update device configured to communicate with a target update device via a network, as in Claims 14 & 22 above, further comprising,

- "the second communication protocol is FTP" (i.e. "transmitting files using the TCP/IP file transfer protocol (FTP). These FTP sites provide the upgrade package for download to client networks which request the upgrade") [column 15 lines 18-21].

Claims 21 & 29:

Frailong et al. disclose a software update method using a software update device configured to and a computer readable storage medium encoded with computer executable instructions, which when executed by a computer, cause the computer to perform a method that controls a software update device configured to communicate with a target update device via a network, as in Claims 14 & 22 above, further comprising,

- "data transmitted via the first communication protocol is encoded" (i.e. "SSL-secured access to the administrative web server") [column 19 lines 43-44];
- "data transmitted via the second communication protocol is not encoded" (i.e. "transmitting files using the TCP/IP file transfer protocol (FTP). These FTP sites provide the upgrade package for download to client networks which request the upgrade") [column 15 lines 18-21].

Claim 30:

Frailong et al. disclose a communication device configured to communicate with a software update device via a network comprising,

- "a certification information setting unit configured to generate a first certification information" (i.e. "Each remote management server receives an RSA key pair along with a public key Certificate signed by the RSA Head-End CA") [column 19 lines 50-52];

- "transmit the first certification information to the software update device via a first communication protocol over the network" (i.e. "The RSA Hardware Certificate 1416 is used in SSL communications where the identity of the gateway interface device needs to be proven, for example when opening a session to a remote management server") [column 19 lines 39-41];
- "a certifying unit configured to execute a certification process, when receiving a second certification information from the software update device, by comparing the first and second certification information" (i.e. "Like the RSA system, the DSA system also includes second and third level key certificates for the gateway interface device") [column 19 lines 61-63];
- "an updating unit configured to receive an update software that updates a software of the communication device from the software update device via a second communication protocol over the network when the certification process succeeds via the first communication protocol" (i.e. "transmitting files using the TCP/IP file transfer protocol (FTP). These FTP sites provide the upgrade package for download to client networks which request the upgrade") [column 15 lines 18-21];
- "update the software of the communication device" (i.e. "If the gateway interface device verifies that an upgrade is both possible and appropriate, the gateway interface device executes the install script to apply the upgrade at the time specified by the apply time window, step 1020") [column 16 lines 14-17];

- "the second communication protocol having a process load less than that of the first communication protocol" (i.e. "transmitting files using the TCP/IP file transfer protocol (FTP). These FTP sites provide the upgrade package for download to client networks which request the upgrade") [column 15 lines 18-21].

Claim 31:

Frailong et al. disclose a communication device configured to communicate with a software update device via a network, as in Claim 30 above, further comprising,

- "a certification information invalidating unit configured to invalidate the first certification information subsequent to the transmittal of the update software" (i.e. "update mechanism using Certificate Revocation Lists. A Certificate Revocation List is a time-valued list of serial numbers signed by a Certification Authority") [column 20 lines 11-13].

Claim 32:

Frailong et al. disclose a communication device configured to communicate with a software update device via a network, as in Claim 30 above, further comprising,

- "a control part configured to instruct an update of the software of the communication device" (i.e. "If the gateway interface device verifies that an upgrade is both possible and appropriate, the gateway interface device executes the install script to apply the upgrade at the time specified by the apply time window, step 1020") [column 16 lines 14-17].

Claim 33:

Frailong et al. disclose a communication device configured to communicate with a software update device via a network, as in Claim 30 above, further comprising,

- "a restarting unit configured to restart the communication device after the software is updated" (i.e. "Once the gateway interface device has executed the upgrade, it performs a reboot so that it boots up in the upgraded state") [column 16 lines 23-25];
- "a start notification transmitting unit configured to transmit a start notification informing that the communication device is started to the software update device when the communication device is started" (i.e. "Once the gateway interface device has executed the upgrade, it performs a reboot so that it boots up in the upgraded state") [column 16 lines 23-25];
- "a version information transmitting unit configured to transmit version information of the communication device in response to a request from the software update device after the start after the transmittal of the start notification" (i.e. "recording the upgraded version number in appropriate places for the configuration manager") [column 16 lines 44-46].

Claim 34:

Frailong et al. disclose a communication device configured to communicate with a software update device via a network, as in Claim 30 above, further comprising,

- "the first communication protocol is SSL" (i.e. "SSL-secured access to the administrative web server") [column 19 lines 43-44].

Claim 35:

Frailong et al. disclose a communication device configured to communicate with a software update device via a network, as in Claim 30 above, further comprising,

- "the second communication protocol is FTP" (i.e. "transmitting files using the TCP/IP file transfer protocol (FTP). These FTP sites provide the upgrade package for download to client networks which request the upgrade") [column 15 lines 18-21].

Claim 36:

Frailong et al. disclose a communication device configured to communicate with a software update device via a network, as in Claim 30 above, further comprising,

- "data transmitted via the first communication protocol is encoded" (i.e. "SSL-secured access to the administrative web server") [column 19 lines 43-44];
- "data transmitted via the second communication protocol is not encoded" (i.e. "transmitting files using the TCP/IP file transfer protocol (FTP). These FTP sites provide the upgrade package for download to client networks which request the upgrade") [column 15 lines 18-21].

Claim 37:

Frailong et al. disclose a software update system comprising,

- "a communication device" (i.e. "remote management server") [column 14 line 64];
- "a software update device in communication with the communication device" (i.e. "gateway interface device") [column 14 line 64];

- "wherein the communication device comprises: a certification information setting unit configured to generate a first certification information" (i.e. "Each remote management server receives an RSA key pair along with a public key Certificate signed by the RSA Head-End CA") [column 19 lines 50-52];
- "transmit the first certification information to the software update device" (i.e. "The RSA Hardware Certificate 1416 is used in SSL communications where the identity of the gateway interface device needs to be proven, for example when opening a session to a remote management server") [column 19 lines 39-41];
- "a certifying unit configured to execute a certification process, when receiving a second certification information from the software update device, by comparing the first and second certification information" (i.e. "Like the RSA system, the DSA system also includes second and third level key certificates for the gateway interface device") [column 19 lines 61-63];
- "an updating unit configured to receive an update software that updates a software of the communication device from the software update device via a second communication protocol over the network when the certification process succeeds via the first communication protocol" (i.e. "transmitting files using the TCP/IP file transfer protocol (FTP). These FTP sites provide the upgrade package for download to client networks which request the upgrade") [column 15 lines 18-21];

- "update the software of the communication device, the second communication protocol having a process load less than that of the first communication protocol" (i.e. "transmitting files using the TCP/IP file transfer protocol (FTP). These FTP sites provide the upgrade package for download to client networks which request the upgrade") [column 15 lines 18-21];
- "wherein the software update device comprises: a memory unit configured to store the first certification information" (i.e. "The gateway interface device stores two root RSA public key certificates and two root DSA public key certificates, with the corresponding private keys") [column 18 lines 57-58];
- "a certification requesting unit configured to transmit the second certification information to the communication device" (i.e. "The second level of certificate key hierarchy for the hardware aspect of the gateway interface device is a manufacturing Certificate Authority, referred to as the RSA Hardware CA 1412") [column 19 lines 18-21];
- "request the communication device to execute the certification process with the first and second certification information" (i.e. "Like the RSA system, the DSA system also includes second and third level key certificates for the gateway interface device") [column 19 lines 61-63];
- "a transmitting unit configured to transmit the update software to the communication device via the second communication protocol over the network when the certification process succeeds" (i.e. "transmitting files using the TCP/IP file transfer protocol (FTP). These FTP sites provide the upgrade package for download to client networks which request the upgrade") [column 15 lines 18-21].

Claim 38:

Frailong et al. disclose a software update system, as in Claim 37 above, further comprising,

- "the communication device further comprises a certification information invalidating unit configured to invalidate the first certification information subsequent to the transmittal of the update software" (i.e. "update mechanism using Certificate Revocation Lists. A Certificate Revocation List is a time-valued list of serial numbers signed by a Certification Authority") [column 20 lines 11-13].

Claim 39:

Frailong et al. disclose a software update system, as in Claim 37 above, further comprising,

- "a restarting unit configured to restart the communication device after the software is updated" (i.e. "Once the gateway interface device has executed the upgrade, it performs a reboot so that it boots up in the upgraded state") [column 16 lines 23-25];
- "a start notification transmitting unit configured to transmit a start notification informing that the communication device is started to the software update device when the communication device is started" (i.e. "Once the gateway interface device has executed the upgrade, it performs a reboot so that it boots up in the upgraded state") [column 16 lines 23-25];
- "a version information transmitting unit configured to transmit version information of the communication device in response to a request from the software update device" (i.e. "recording the upgraded version number in appropriate places for the configuration manager") [column 16 lines 44-46];

- "wherein the software update device further has a version information unit configured to obtain the version information by requesting the communication device to transmit the version information when the start notification is received after the transmittal of the update software" (i.e. "recording the upgraded version number in appropriate places for the configuration manager") [column 16 lines 44-46];
- "confirming the update by comparing with version information of the transmitted update software" (i.e. "recording the upgraded version number in appropriate places for the configuration manager") [column 16 lines 44-46].

Claim 40:

Frailong et al. disclose a software update system, as in Claim 37 above, further comprising,

- "the first communication protocol is SSL" (i.e. "SSL-secured access to the administrative web server") [column 19 lines 43-44].

Claim 41:

Frailong et al. disclose a software update system, as in Claim 37 above, further comprising,

- "the second communication protocol is FTP" (i.e. "transmitting files using the TCP/IP file transfer protocol (FTP). These FTP sites provide the upgrade package for download to client networks which request the upgrade") [column 15 lines 18-21].

Claim 42:

Frailong et al. disclose a software update system, as in Claim 37 above, further comprising,

- "data transmitted via the first communication protocol is encoded" (i.e. "SSL-secured access to the administrative web server") [column 19 lines 43-44];

- "data transmitted via the second communication protocol is not encoded" (i.e. "transmitting files using the TCP/IP file transfer protocol (FTP). These FTP sites provide the upgrade package for download to client networks which request the upgrade") [column 15 lines 18-21].

Claims 43 & 50:

Frailong et al. disclose a software update method using a communication device configured to and a computer readable storage medium encoded with computer executable instructions, which when executed by a computer, cause the computer to perform a method that controls a communication device configured to communicate with a software update device via a network comprising,

- "generating a first certification information" (i.e. "Each remote management server receives an RSA key pair along with a public key Certificate signed by the RSA Head-End CA") [column 19 lines 50-52];
- "transmitting the first certification information to the software update device via a first communication protocol over the network" (i.e. "The RSA Hardware Certificate 1416 is used in SSL communications where the identity of the gateway interface device needs to be proven, for example when opening a session to a remote management server") [column 19 lines 39-41];
- "executing a certification process, when receiving a second certification information from the software update device, by comparing the first and second certification information" (i.e. "Like the RSA system, the DSA system also includes second and third level key certificates for the gateway interface device") [column 19 lines 61-63];

- "receiving an update software that updates a software of the communication device from the software update device via a second communication protocol over the network when the certification process succeeds via the first communication protocol" (i.e. "transmitting files using the TCP/IP file transfer protocol (FTP). These FTP sites provide the upgrade package for download to client networks which request the upgrade") [column 15 lines 18-21];
- "updating the software of the communication device" (i.e. "If the gateway interface device verifies that an upgrade is both possible and appropriate, the gateway interface device executes the install script to apply the upgrade at the time specified by the apply time window, step 1020") [column 16 lines 14-17];
- "the second communication protocol having a process load less than that of the first communication protocol" (i.e. "transmitting files using the TCP/IP file transfer protocol (FTP). These FTP sites provide the upgrade package for download to client networks which request the upgrade") [column 15 lines 18-21].

Claims 44 & 51:

Frailong et al. disclose a software update method using a communication device configured to and a computer readable storage medium encoded with computer executable instructions, which when executed by a computer, cause the computer to perform a method that controls a communication device configured to communicate with a software update device via a network, as in Claims 43 & 50 above, further comprising,

- "a step of invalidating the first certification information subsequent to the transmittal of the update software" (i.e. "update mechanism using Certificate Revocation Lists. A Certificate Revocation List is a time-valued list of serial numbers signed by a Certification Authority") [column 20 lines 11-13].

Claims 45 & 52:

Frailong et al. disclose a software update method using a communication device configured to and a computer readable storage medium encoded with computer executable instructions, which when executed by a computer, cause the computer to perform a method that controls a communication device configured to communicate with a software update device via a network, as in Claims 43 & 50 above, further comprising,

- "a step of updating the software in response to an instruction to update the software from a control part" (i.e. "If the gateway interface device verifies that an upgrade is both possible and appropriate, the gateway interface device executes the install script to apply the upgrade at the time specified by the apply time window, step 1020") [column 16 lines 14-17].

Claims 46 & 53:

Frailong et al. disclose a software update method using a communication device configured to and a computer readable storage medium encoded with computer executable instructions, which when executed by a computer, cause the computer to perform a method that controls a communication device configured to communicate with a software update device via a network, as in Claims 43 & 50 above, further comprising,

- "restarting the communication device after the software is updated" (i.e. "Once the gateway interface device has executed the upgrade, it performs a reboot so that it boots up in the upgraded state") [column 16 lines 23-25];
- "transmitting a start notification informing that the communication device is started to the software update device when the communication device is started" (i.e. "Once the gateway interface device has executed the upgrade, it performs a reboot so that it boots up in the upgraded state") [column 16 lines 23-25];
- "transmitting version information of the communication device in response to a request from the software update device after the start after the transmittal of the start notification" (i.e. "recording the upgraded version number in appropriate places for the configuration manager") [column 16 lines 44-46].

Claims 47 & 54:

Frailong et al. disclose a software update method using a communication device configured to and a computer readable storage medium encoded with computer executable instructions, which when executed by a computer, cause the computer to perform a method that controls a communication device configured to communicate with a software update device via a network, as in Claims 43 & 50 above, further comprising,

- "the first communication protocol is SSL" (i.e. "SSL-secured access to the administrative web server") [column 19 lines 43-44].

Claims 48 & 55:

Frailong et al. disclose a software update method using a communication device configured to and a computer readable storage medium encoded with computer executable instructions, which when executed by a computer, cause the computer to perform a method that controls a communication device configured to communicate with a software update device via a network, as in Claims 43 & 50 above, further comprising,

- "the second communication protocol is FTP" (i.e. "transmitting files using the TCP/IP file transfer protocol (FTP). These FTP sites provide the upgrade package for download to client networks which request the upgrade") [column 15 lines 18-21].

Claims 49 & 56:

Frailong et al. disclose a software update method using a communication device configured to and a computer readable storage medium encoded with computer executable instructions, which when executed by a computer, cause the computer to perform a method that controls a communication device configured to communicate with a software update device via a network, as in Claims 43 & 50 above, further comprising,

- "data transmitted via the first communication protocol is encoded" (i.e. "SSL-secured access to the administrative web server") [column 19 lines 43-44];
- "data transmitted via the second communication protocol is not encoded" (i.e. "transmitting files using the TCP/IP file transfer protocol (FTP). These FTP sites provide the upgrade package for download to client networks which request the upgrade") [column 15 lines 18-21].

Response to Arguments

3. Applicant's arguments with respect to Claims 1-56 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

4. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Thursday from 7:30 AM to 4:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at 571-272-4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

OAL
03/05/2008

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2136